



NEWSLETTER

N° 3 - 14 mars 2006

Il est possible de [souscrire un abonnement](#) à la Newsletter trimestrielle du CEPD sur notre site Internet.

www.edps.eu.int

Sommaire:

1. Le [principe de disponibilité](#) - Avis du CEPD sur la proposition de décision-cadre
2. [Interopérabilité des bases de données](#) - Commentaires du CEPD sur la communication de la Commission
3. Rapport d'inspection d'[Eurodac](#)
4. Informations concernant le [contrôle préalable](#) par le CEPD de traitements de données à caractère personnel
5. Nouveaux [délégués à la protection des données](#)
6. [Nouveau logo](#) du CEPD
7. [Colophon](#)

1. Le principe de disponibilité - Avis du CEPD sur la proposition de décision-cadre

Le Contrôleur européen de la protection des données (CEPD) a récemment présenté son avis sur la proposition de décision-cadre relative à l'échange d'informations en vertu du principe de disponibilité. Introduit par le programme de la Haye, ce principe signifie que les informations disponibles pour les autorités des services répressifs d'un État membre doivent l'être aussi pour les autorités équivalentes dans les autres États membres. Ce principe soulève un certain nombre de questions en matière de

protection des données, en raison notamment de la sensibilité des données et du contrôle réduit de l'usage des informations.

Dans son avis, le CEPD préconise une introduction progressive et prudente du principe de disponibilité en raison des risques importants que comporte le partage de données sensibles. Il prône l'utilisation d'un seul type de données (et non de six comme le propose la Commission), l'accès indirect (données d'index renvoyant à des informations auxquelles on ne peut pas accéder en ligne) et un système "hit - no hit", qui permettrait un plus grand contrôle de l'échange d'informations qu'un système basé sur l'accès direct.

Cliquez ici pour lire [l'avis](#) ou le [communiqué de presse](#).

2. Interopérabilité des bases de données - Observations du CEPD sur la communication de la Commission

Le CEPD a transmis à la Commission ses observations sur les différents scénarios envisageables concernant l'interopérabilité des bases de données dans le domaine de la Justice et des Affaires intérieures, que la Commission avait présentés dans l'une de ses communications. L'interopérabilité soulève un certain nombre de questions en matière de protection des données, puisqu'elle permettra un nouvel accès aux données à caractère personnel des citoyens de l'Union européenne. Le CEPD est par conséquent en profond désaccord avec la Commission, qui considère l'interopérabilité comme un concept technique plutôt que juridique ou politique, et en appelle à un examen attentif en la matière.

Dans les observations qu'il a adressées à la Commission, le CEPD a fermement déconseillé l'utilisation des données biométriques, telles que les empreintes digitales - ou même l'ADN - comme clé d'identification unique (la référence à une personne). La précision de la biométrie est surestimée dans ce contexte et facilitera des interconnexions injustifiées de bases de données.

Cette communication a conduit le CEPD à créer un nouvel outil ("Observations") pour présenter ses points de vue. Plus brèves et moins complètes que les avis, les observations du CEPD seront entre autres utilisées pour traiter des communications de la Commission susceptibles, à long terme, d'avoir des incidences stratégiques sur la protection des données à caractère personnel.

Cliquez ici pour lire les [observations](#) ou le [communiqué de presse](#).

3. Rapport d'inspection d'Eurodac

Le CEPD a récemment conduit sa première inspection de l'unité centrale d'Eurodac et établi un rapport dans lequel il se montre globalement satisfait du niveau de sécurité. Il a néanmoins formulé un certain nombre de recommandations concrètes.

Le système Eurodac, dans lequel sont enregistrées les empreintes digitales de tous les demandeurs d'asile de l'UE, est utilisé par les États membres dans le cadre de la procédure d'asile. Une bonne protection des données est d'une importance capitale

pour les demandeurs d'asile de même que pour le bon fonctionnement du système, qui se compose d'une unité centrale ainsi que d'unités locales situées dans les États membres.

L'unité centrale est gérée par l'Union européenne et supervisée par le CEPD. La première inspection du CEPD a porté sur plusieurs aspects de la sécurité, comme la gestion des risques et des incidents, la sécurité des communications et le contrôle des accès physiques aux installations. Il sera suivi d'un audit de sécurité approfondi qui doit se dérouler mi-2006. Compte tenu du partage de responsabilités entre le CEPD et les autorités responsables de la protection des données dans les États membres (lesquels sont responsables au niveau national), il est important d'adopter une approche commune du contrôle. Le CEPD a donc organisé une réunion de coordination et présentera son rapport d'inspection lors de la prochaine réunion prévue en juin.

Cliquez ici pour lire le [communiqué de presse](#).

4. Informations concernant le contrôle préalable par le CEPD de traitements de données à caractère personnel

Le traitement des données à caractère personnel par l'administration de l'UE qui est susceptible de présenter des risques particuliers pour certaines personnes (les personnes concernées) fait l'objet d'un contrôle préalable par le CEPD. Cette procédure sert à déterminer si le traitement est conforme ou non au règlement (CE) n° 45/2001 sur la protection des données, qui définit les obligations des institutions et des organes de l'UE en matière de protection des données. Les avis sont publiés sur le site du CEPD. Trois avis récents concernent:

La procédure de sélection EPSO

L'Office européen de sélection du personnel (EPSO) assure le recrutement de fonctionnaires par voie de concours. Dans son avis, le CEPD a jugé nécessaire de souligner que les données à caractère personnel ne se limitent pas aux données personnelles d'identification, mais englobent toutes les données qui concernent une personne identifiée ou identifiable - ce qui est le cas lorsque les données ont trait à l'identité ou au comportement d'une personne ou lorsqu'elles sont utilisées dans un but d'évaluation. Ceci est important dans le cadre des concours, mais aussi dans celui des appréciations personnelles du jury.

Pour l'essentiel, EPSO a suivi les principes du règlement. Le CEPD a néanmoins formulé quelques recommandations concernant la durée de conservation, la conservation à long terme des données et la limitation de la transmission des données aux seuls services chargés du recrutement. Il a en outre fait une recommandation particulière sur la publication des conditions des concours au Journal officiel: domaine sur lequel portent les épreuves orales, détail des notes obtenues - et information des candidats sur leur droit d'accès aux résultats des épreuves orales.

Horaire flexible

Le Secrétariat général du Conseil (SGC) compte introduire un système informatique pour enregistrer et gérer les heures de travail et les absences de son personnel, afin de gérer les règles relatives à l'horaire flexible. L'enregistrement, qui se fera en

présentant son badge aux lecteurs installés près des entrées, et l'utilisation d'intranet (enregistrement et validation/autorisation par le supérieur hiérarchique direct) font partie du système, qui sera connecté aux bases de données des services des ressources humaines.

Dans son avis, le CEPD a conclu que le système était conforme au règlement, pour autant que certaines recommandations soient prises en considération. Ces recommandations concernent par exemple la durée de conservation des données, la définition de l'accès des supérieurs aux données à caractère personnel des membres du personnel se trouvant sous leur responsabilité et les informations devant être transmises aux personnes concernées.

Lignes téléphoniques et radios de sécurité du Conseil

Toute personne témoin d'un accident ou d'un incident se produisant dans les bâtiments du Conseil doit en informer le Centre de sécurité. Le témoin, qui normalement prévient le Centre de sécurité par téléphone, doit mentionner son nom ainsi que le lieu et le motif de son appel. Le fonctionnaire chargé de la sécurité notifiera immédiatement le service d'urgence compétent. Par la suite, un nombre restreint de personnes peut écouter les communications enregistrées, si cela est nécessaire pour déterminer le cours exact des événements dans les actions de suivi, pour analyser les messages de menace transmis par téléphone ou pour vérifier la conformité avec les instructions internes du Bureau de sécurité.

Dans son avis, le CEPD conclut que le règlement est respecté, pour autant que certaines recommandations soient prises en considération, par exemple en ce qui concerne l'interprétation stricte de la limitation du droit d'accès des personnes concernées.

Cliquez [ici](#) pour l'index renvoyant aux versions intégrales des avis.

5. Nouveaux délégués à la protection des données

Chaque institution ou organe de l'UE est obligé de désigner au moins un délégué à la protection des données (DPD). Ceux-ci doivent veiller de manière indépendante à l'application interne du règlement (CE) n°45/2001. Le CEPD a publié un [document de référence](#) sur le rôle joué par les DPD, qui a reçu un écho positif et a augmenté le nombre des DPD.

Récentes nominations:

Loïc Julien, médiateur européen

Laraine Laudati, Office européen de lutte antifraude

Romuald Delli Paoli, Fondation européenne pour la formation

Andreas Mitrakas, Agence européenne chargée de la sécurité des réseaux et de l'information

Arne Tvedt, Observatoire européen des drogues et des toxicomanies

Claus Reunis, Autorité européenne de sécurité des aliments

La liste complète des DPD est disponible [ici](#).

6. Nouveau logo CEPD

La création d'un nouveau logo du CEPD, mettant en évidence le lien du CEPD avec les "institutions de l'UE" tout en soulignant son indépendance, a été achevée fin 2005.

Le nouveau logo, qui contient des références visuelles claires aux principales responsabilités du CEPD est progressivement introduit en 2006.

Reprenant le jaune et le bleu du drapeau européen, le logo du CEPD a la forme d'un disque de stockage de données en mouvement, lequel peut également être interprété comme un bouclier protégeant les données. L'ellipse formée par les pixels d'informations représente une silhouette qui se transforme peu à peu en étoiles européennes.

7. Colophon

Cette Newsletter est publiée par le Contrôleur européen de la protection des données, une autorité européenne indépendante, créée en 2004 pour:

- contrôler le traitement des données personnelles dans les administrations de l'UE;
- conseiller sur la législation en matière de protection des données;
- coopérer avec les autorités similaires afin de garantir la cohérence de la protection des données.

Adresse postale:
EDPS - CEPD
Rue Wiertz 60 - MO 63
B-1047 Bruxelles
BELGIQUE

Bureaux:
Rue Montoyer 63
Bruxelles
BELGIQUE

Coordonnées:
Tél: +32 (0)2 283 19 00
Fax: +32 (0)2 283 19 50
Courriel: edps@edps.eu.int

CEPD - le gardien européen de la protection des données personnelles

www.edps.eu.int